

PATENT COOPERATION TREATY

5

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 20 October 2000 (20.10.00)	
International application No. PCT/US00/02174	Applicant's or agent's file reference 18926-39PC
International filing date (day/month/year) 28 January 2000 (28.01.00)	Priority date (day/month/year) 29 January 1999 (29.01.99)
Applicant MEDVINSKY, Sasha et al	

1. The designated Office is hereby notified of its election made:



in the demand filed with the International Preliminary Examining Authority on:

25 August 2000 (25.08.00)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Antonia Muller Telephone No.: (41-22) 338.83.38
---	--

PCT

REC'D 08 MAY 2001

WIPO

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 18926-39PC	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/US00/02174	International filing date (day/month/year) 28 January 2000 (28.01.2000)	Priority date (day/month/year) 29 January 1999 (29.01.1999)
International Patent Classification (IPC) or national classification and IPC IPC(7): H04K 1/00 and US Cl.: 713/153		
Applicant GENERAL INSTRUMENT CORPORATION		
<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>3</u> sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of <u>0</u> sheets.</p> <p>3. This report contains indications relating to the following items:</p> <ul style="list-style-type: none"> I <input checked="" type="checkbox"/> Basis of the report II <input type="checkbox"/> Priority III <input type="checkbox"/> Non-establishment of report with regard to novelty, inventive step and industrial applicability IV <input type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input type="checkbox"/> Certain documents cited VII <input type="checkbox"/> Certain defects in the international application VIII <input type="checkbox"/> Certain observations on the international application 		
Date of submission of the demand 25 August 2000 (25.08.2000)	Date of completion of this report 13 April 2001 (13.04.2001)	
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gilberto Barron Jr. <i>Peggy Harwood</i> Telephone No. (703) 305-3900	

Form PCT/IPEA/409 (cover sheet)(July 1998)

I. Basis of the report**1. With regard to the elements of the international application:***

- ☒ the international application as originally filed.
- ☒ the description:
pages 1-8 _____ as originally filed
pages NONE _____, filed with the demand
pages NONE _____, filed with the letter of _____.
- ☒ the claims:
pages 9-11 _____, as originally filed
pages NONE _____, as amended (together with any statement) under Article 19
pages NONE _____, filed with the demand
pages NONE _____, filed with the letter of _____.
- ☒ the drawings:
pages 1-5 _____, as originally filed
pages NONE _____, filed with the demand
pages NONE _____, filed with the letter of _____.
- ☒ the sequence listing part of the description:
pages NONE _____, as originally filed
pages NONE _____, filed with the demand
pages NONE _____, filed with the letter of _____.

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in printed form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

- ☒ the description, pages NONE
- ☒ the claims, Nos. NONE
- ☒ the drawings, sheets/fig NONE

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. STATEMENT**

Novelty (N)	Claims <u>1-10</u>	YES
	Claims <u>NONE</u>	NO
Inventive Step (IS)	Claims <u>NONE</u>	YES
	Claims <u>1-10</u>	NO
Industrial Applicability (IA)	Claims <u>1-10</u>	YES
	Claims <u>NONE</u>	NO

2. CITATIONS AND EXPLANATIONS (Rule 70.7)

Claims 1-4 and 6-9 lack an inventive step under PCT Article 33(3) as being obvious over Ross, Jr. (hereinafter, "Ross") (U.S. 5,812,671).

Ross discloses a method for establishing a secure communication channel comprising receiving a request at the first gateway controller to establish a secure communication channel between the first user and the second user; generating a secret key at the first gateway controller; distributing the secret key; and establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key (see fig. 1 and associated text). Ross does not explicitly disclose the environment of an IP telephony network; however, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Ross to work in such a telephone environment.

Claims 5 and 10 lack an inventive step under PCT Article 33(3) as being obvious over Ross, Jr. (hereinafter, "Ross") (U.S. 5,812,671) in view of Schneier in *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed.

Ross does not explicitly disclose the aspect of key escrow. However, Schneier teaches key escrow. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Ross to deal with key escrow by incorporating the teachings of Schneier.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US00/02174

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04K 001/00

US CL : 713/153

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : Please See Continuation Sheet

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,999,525 A (KRISHNASWAMY et al) 07 December 1999 (01.12.1999), entire document	1-10
A	US 5,410,602 A (FINKELSTEIN et al) 25 April 1995 (25.04.1995), figs. 2-3 and associated text.	1-10
A	US 5,539,824 A (BJORKLUND et al) 23 July 1996 (23.07.1996), see abstract and background.	1-10
A	US 5,825,888 A (KIMURA et al) 20 October 1998 (20.10.1998), see fig. 1 and associated	1-10
Y	SCHNEIER, BRUCE. Applied Cryptography: Protocols, Algorithms, and Source Code in C. October 1995, pages 97-100 and 181-182.	5,10
Y,P	US 5,974,043 A (SOLOMON) 26 October 1999 (26.10.1999), see background and figs. 1 & 2 and associated texts.	1-10
Y	US 5,812,671 A (ROSS, JR.) 22 September 1998 (22.09.1998), figs 1& 3 and associated	1-10
Y	US 5,371,794 A (DIFFIE et al) 06 December 1994 (06.12.1994), fig. 2 and associated	1-10
Y	US 5,600,722 A (YAMAGUCHI et al) 04 February 1997 (04.02.1997), see figs. 3, 9, and 15 associated texts.	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

05 May 2000 (05.05.2000)

Date of mailing of the international search report

12 JUN 2000

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Gail O. Hayes

Telephone No. 703 306-5539

James R. Matthews

INTERNATIONAL SEARCH REPORT

International application No.

PCT/ISA00/02174

Continuation of B. FIELDS SEARCHED Item 1: 370/352, 389, 392; 379/90.01, 93.01, 93.08-93.09, 900; 380/243, 247, 260, 270, 276, 278, 286; 709/205, 227-228; 713/150-153

Continuation of B. FIELDS SEARCHED Item 3: BRS [((ip or internet) adj telephon\$) and (encrypt\$ or encipher\$ or security)] and [(gateway) same (encrypt\$ or encipher\$ or security)]